

# General Data Protection Regulation (GDPR)

## Privacy Policy

### 1. Introduction

At **AAAAAA** (“we,” “our,” or “us”), we recognize the importance of protecting your personal data. This Privacy Policy outlines how we collect, use, store, and protect your personal data when you use our software, **Appointment System**. We are committed to complying with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and ensuring that your privacy rights are respected and safeguarded.

The **Appointment System** is designed to facilitate the arrangement of medical appointments between patients and doctors. We take all necessary measures to ensure that personal data is handled in a secure and lawful manner. This Privacy Policy details how we collect and process personal data to provide our services, as well as your rights under the GDPR.

### 2. Personal Data We Collect

We collect personal data that is necessary to deliver our appointment scheduling services. The following types of personal data may be collected and processed:

- **Required Personal Data:**
  - Name
  - Surname
  - Email Address
  - Phone Number
  - Gender
  - Date of Birth (Age)
- **Optional Data Removed (Not Collected Anymore):**
  - Address
  - Postal Code
  - City
  - ID Number

This data is primarily provided by the doctor or the doctor’s secretary, and is used exclusively for managing appointments, notifications, and providing analytics. We do **not** collect sensitive personal health data such as medical history, insurance details, or diagnoses.

### 3. Purpose of Data Collection

The primary purpose of collecting personal data is to provide our appointment management services and to communicate with patients and doctors effectively. We process personal data for the following reasons:

- **Appointment Scheduling:** The software enables doctors and patients to schedule, manage, and confirm appointments.
- **Notification Services:** We use email and phone numbers to send appointment confirmations, reminders, and other notifications relevant to patients' appointments.
- **Data Analytics:** We analyze the collected data (age and gender) to help doctors and the system administrators gain insights into usage patterns and improve the system.

We do not use personal data for marketing, advertising, or any other purposes outside of the primary services provided by the software.

## 4. Data Storage and Security Measures

We take data security seriously and use industry-standard security measures to protect personal data. The data we collect is securely stored on cloud-based servers that are located in Europe.

### Hosting Providers and Locations:

- **Contabo VPS (Europe)**
- **Velia (France, EU)**

These hosting providers ensure that all data remains in the EU, complying with GDPR regulations. We also ensure that all third-party service providers comply with GDPR and that your personal data is treated with the highest level of security.

### How Data is Stored:

- All personal data is stored on a **cloud-based server**.
- The data is entered into the system by the **doctor or the doctor's secretary**.
- **Patients cannot directly input or modify their own data** within the software.

### Data Protection Measures:

- **Encryption:** All data stored in our system, including databases and hard drives, is encrypted to prevent unauthorized access.
- **Access Control:** Only authorized personnel can access the server, and the server itself is only accessible from our office for maintenance purposes.
- **SSL Encryption:** We use Secure Socket Layer (SSL) encryption for all data transmissions, ensuring that data is securely transmitted between the user and the server.

- **Authentication:** We require users (doctors and secretaries) to log in with **username** and **password** credentials to access the system.

## 5. Sharing Personal Data with Third Parties

We do not sell or share personal data with third parties for marketing purposes. However, we do share personal data with certain trusted third-party service providers in order to operate the software and provide essential services. These include:

Third-Party Provider	Purpose of Data Sharing	Location
Velia.net Internetdienste GmbH	Cloud Hosting Services	Germany
Contabo GmbH	Cloud Hosting Services	Germany
Cytacom Solutions Ltd	SMS Notification Service	Cyprus
Databasemart LLC	Email Notification Service	USA

We ensure that all third-party providers comply with GDPR and that any data shared with them is handled securely and lawfully. All third-party providers are contractually obligated to maintain the confidentiality of your data.

## 6. User Rights Under GDPR

As a user, you have various rights regarding your personal data under the GDPR. These rights include:

1. **Right to Access:** You have the right to request access to your personal data that we hold.
2. **Right to Rectification:** You can request correction of any inaccurate or incomplete data we have about you.
3. **Right to Erasure (Right to be Forgotten):** You can request that we delete your personal data under certain conditions.
4. **Right to Restriction of Processing:** You can ask us to restrict the processing of your data in certain situations.
5. **Right to Data Portability:** You can request a copy of your personal data in a structured, commonly used format, which you can transfer to another service.
6. **Right to Object:** You can object to our processing of your personal data for certain purposes, including data processing that is based on legitimate interests or is for direct marketing purposes.

### Exercising Your Rights:

- Currently, patients **cannot directly modify or delete** their personal data through the software.

- If you wish to exercise your rights (e.g., access, rectification, or deletion of your data), please contact us at **[Insert Contact Information]**. We will respond to your request within the timeframe specified by the GDPR.
- Additionally, we offer a **GDPR Report** feature within the software, allowing doctors or their secretaries to generate a PDF report detailing the data stored about a patient. This report can be provided to patients upon their request.

## 7. Data Retention

We retain personal data as long as it is necessary to provide our services and comply with legal obligations.

- **Data Retention Period:** We do not currently have an automatic system in place for deleting or anonymizing data. The data is kept until the patient no longer requires appointments with the doctor.
- **Patient Data:** If patients request the deletion of their data, we will comply within the limits of applicable law.

We are reviewing our **data retention policy** to ensure compliance with GDPR guidelines and to implement automatic data deletion or anonymization procedures where necessary.

## 8. Legal Basis for Data Processing

Under the GDPR, we must have a legal basis to collect and process your personal data. Currently, the data is entered into the software by the doctor or the doctor's secretary, and we are assessing the most appropriate legal basis for processing this data. Possible legal bases include:

- **User Consent:** If we require consent to collect data, we will implement a consent mechanism within the software.
- **Contractual Necessity:** The processing of personal data may be necessary to provide the appointment scheduling services that the patient has requested.
- **Legal Obligation:** We may be required to process certain data to comply with legal obligations related to healthcare.

We are evaluating the need for **written consent** from patients for data processing and will implement such consent mechanisms in the future if necessary.

## 9. Cookies and Tracking Technologies

The **Appointment System** does not use cookies or any tracking technologies for user behavior analysis or advertising purposes. The software is operated on a **subscription model for doctors**,

and we do not track or monitor users' activities beyond the appointment scheduling functionality.

## 10. Data Transfers Outside the EU

We ensure that all personal data is stored within the **European Union (EU)**. However, some of our third-party providers, such as **Databasemart LLC (USA)**, may process personal data outside the EU. We ensure that all third-party service providers comply with GDPR requirements by using appropriate safeguards, such as:

- **Standard Contractual Clauses (SCCs):** We enter into contracts with our service providers to ensure that they comply with GDPR requirements for data transfers outside the EU.

## 11. GDPR Report Feature

As part of our commitment to GDPR compliance and transparency, we have implemented a **GDPR Report** feature within the **Appointment System**. This feature enables doctors or their secretaries to generate a detailed **PDF report** containing the personal data that is stored for each patient. This report can be provided to the patient upon request, ensuring that patients can access and review the data we hold about them.

## 12. Contact Information

For any questions, concerns, or requests regarding this Privacy Policy or your personal data, please contact us at:

**AAAAAA**

**BBBBBB**

**Email:** CCC@gmail.com

**Phone:** +357912121212